AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Northern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

(1) A GOOGLE PIXEL 6A CELL PHONE; AND (2) AN HP ELITEBOOK LAPTOP COMPUTER, FURTHER DESCRIBED IN ATTACHMENT A.

Case No. 8:24-MJ-511 (GLF)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

(1) A GOOGLE PIXEL 6A CELL PHONE; AND (2) AN HP ELITEBOOK LAPTOP COMPUTER, FURTHER DESCRIBED IN ATTACHMENT A.

located in the Northern District of New York, there is now concealed *(identify the person or describe the property to be seized):*

SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 8, United States Code, Section 1326(a) and (b)(2)	Illegal Re-Entry of a Removed Alien with a Prior Conviction for an Aggravated Felony

The application is based on these facts:

See Attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Benjamin W. LaBaff, Border Patrol Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: Nov. 5, 2024

Judge's signature

City and state: Plattsburgh, NY

Hon. Gary L. Favro, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF: (1) A GOOGLE PIXEL 6A CELL PHONE; AND (2) AN HP ELITEBOOK LAPTOP COMPUTER	Case No. 8:24-MJ-511 (GLF)

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Benjamin W. LaBaff, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of two electronic devices and the extraction of electronically stored information from those devices. The devices in question are one (1) Google Pixel 6A ("Device A"); and one (1) HP Elitebook Laptop ("Device B") (collectively, the "Subject Devices"). The Subject Devices are currently in the custody of the United States Border Patrol at 135 Trippany Road, Massena, New York 13662. The description of the property to be searched is described in the following paragraphs and in Attachment A. The evidence sought is described in Attachment B.

2. I am a Border Patrol Agent ("BPA") with the United States Department of Homeland Security ("DHS"), Bureau of Customs and Border Protection ("CBP"), United States Border Patrol, and assigned to the Massena Border Patrol Station. I have been a Border Patrol Agent since December 2008. My primary duty is to assist in the prevention of illicit trafficking of people and contraband between official ports of entry. My authority to perform this mission is articulated in the Immigration and Nationality Act, sections 235 and 287, and Title 8, United States Code, Section 1357. These bodies of law relate to, among other things, a Border Patrol Agent's

authority to interrogate any alien or person believed to be an alien, and to make an arrest of any alien who is entering or attempting to enter the United States in violation of the immigration laws. To enforce these laws, I have received training at the Federal Law Enforcement Training Center in Artesia, New Mexico in law, operations, firearms, driving techniques, and physical techniques.

3. I have investigated violations of the Immigration Nationality Act ("INA") including illegal entry of aliens in violation of Title 8, United States Code, Section 1325; the smuggling of aliens in violation of Title 8, United States Code, Section 1324; and the illegal re-entry of aliens in violation of Title 8, United States Code, Section 1326. I have written and executed search warrants for electronic devices and have reviewed the evidence contained within. I have analyzed data and information from electronic devices and presented that data as evidence during criminal investigations.

4. The statements and facts set forth in this affidavit are based in significant part on the following: a review of Border Patrol reports; my discussions with other investigators and BPAs involved in this investigation; my own involvement in this investigation; and my training and experience as a BPA. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

5. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that Paul MALAGERIO ("MALAGERIO") has committed a violation of Title 8, United States Code, Section 1326(a) and (b)(2) (illegal re-entry of a removed alien with a prior conviction for an aggravated felony) (the "Target Offense"), and that evidence of that violation is located inside the Subject Devices. There is also probable cause to search the Subject Devices, as described in Attachment A, for evidence, instrumentalities, contraband, and/or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

6. On October 27, 2024, Royal Canadian Mounted Police ("RCMP") notified United States Border Patrol Agents that an individual had been observed on a bicycle near the border of Canada and the United States in the proximity of Burns Holden Road in Franklin County, New York. Approximately an hour later, Massena Border Patrol Agents encountered the defendant, Paul MALAGERIO, a native and citizen of Canada, on foot at a location in between Burns Holden Road and New York State Highway 37 near Fort Covington, Franklin County, New York. The specific area where MALAGERIO was encountered is a cleared area situated underneath power lines that runs approximately north to south in between Burns Holden Road and Highway 37. This cleared area underneath the power lines where MALAGERIO was encountered has seen a major increase in foot traffic related to illegal entries over the past year. Border Patrol Agents have apprehended numerous individuals who have entered the United States illegally at this location.

7. After being detained, MALAGERIO readily admitted to being in the United States illegally. BPAs searched MALAGERIO's person and belongings and discovered Device A on his person and Device B in his backpack. BPAs seized the Subject Devices, and MALAGERIO was transported to the Massena Border Patrol Station.

8. Upon arrival at the Border Patrol Station, MALAGERIO was fingerprinted. A review of law enforcement records revealed that MALAGERIO had been ordered removed from the United States on December 13, 2022, and had been actually removed from the United States from Atlanta, Georgia, on February 16, 2023. Court records also revealed that on March 2, 2021, MALAGERIO had been convicted of the federal offense of Possession of a Weapon by an Illegal Alien pursuant to 18 U.S.C. §§ 922(g)(5) and 924(a)(2) in the Northern District of Texas. On July 15, 2021, he was sentenced to 28 months imprisonment and 12 months supervised release for that

offense. A conviction for a violation of 18 U.S.C. § 922(g)(5) qualifies as an "aggravated felony" pursuant to 8 U.S.C. § 1326(b)(2). MALAGERIO's February 16, 2023, removal from the United States was subsequent to his aggravated felony conviction.

9. On October 30, 2024, MALAGERIO was charged by complaint with a violation of Title 8, United States Code, Section 1326(a) and (b)(2) (illegal reentry by removed alien with prior aggravated felony conviction).

10. Based on my training and experience in this and other cross-border criminal investigations I have been involved with, including other investigations involving individuals entering the United States illegally, individuals who illegally cross the border will often communicate and coordinate with individuals in the United States to arrange for someone to pick them up once they have successfully crossed the border, or to inform individuals in the United States or in their country of origin that they successfully crossed the border. Based on my training and experience, this communication and coordination is frequently facilitated via cellular telephone. Additionally, individuals involved in crossing the border illegally often use a cellular telephone's GPS function to search for and map out potential crossing and pickup locations and to navigate to such places. An additional function of cellular telephones that can be utilized by individuals crossing illegally includes the camera, as individuals will often take photos of where they crossed the border illegally. Based on my training and experience, such photographs are used to assist future smugglers, border-crossers, or the picture-takers themselves if they seek to cross the border again at a later time.

11. Additionally, based on my training and experience, smugglers often communicate with one another using cell phones and downloaded applications to coordinate smuggling events. Smartphones, such as the Subject Devices, can also be used to access social media. Based on my

training, knowledge, and experience of alien smuggling, I know that social media platforms, such as Facebook, are often used by smugglers to find customers and for communication between smugglers and aliens illegally entering the United States.

TECHNICAL TERMS

12. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. They may also have removable storage media connected to them or stored with them, including micro-SD cards or other types of memory cards.

b. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer that accesses the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

c. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

e. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video,

or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

f. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

g. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices

and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

13. Based on my training, experience, and research, I know that the Subject Devices are the type of electronic devices that have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Also, due to the nature and circumstances of the offense in this case, it is reasonable to expect that records relating to communications MALAGERIO engaged in with individuals in Canada or the United States to facilitate MALAGERIO's border crossing or pickup once in the United States may be found on the devices.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, certain information from webpages and media that has been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

15. There is probable cause to believe that things that were once stored on the Subject Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the Target Offense, but also forensic evidence that establishes how the Subject Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection, in order to determine whether it is evidence described by the warrant. The examination will be performed by representatives from the Department of Homeland Security and their designees.

18. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Additionally, it is unclear at this time what hours the government employee(s) who will be doing the examinations of these Subject Devices will be working at the time they perform them. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. Based on the foregoing information, there is probable cause to believe that MALAGERIO has violated Title 8, United States Code, Section 1326(a) and (b)(2) (illegal re-entry of a removed alien with a prior conviction for an aggravated felony). I respectfully request that a warrant be issued authorizing the search of the Subject Devices for evidence, instrumentalities, contraband, and/or fruits of that offense.

ATTESTED TO BY THE APPLICANT IN ACCORDANCE WITH THE REQUIREMENTS OF RULE 4.1 OF THE FEDERAL RULES OF CRIMINAL PROCEDURE

Benjamin W. LaBaff
Border Patrol Agent
United States Border Patrol

I, the Honorable Gary L. Favro, United States Magistrate Judge, hereby acknowledge that this affidavit was attested by the affiant by telephone on Nov. 5, 2024, in accordance with Rule 4.1 of the Federal Rules of Criminal Procedure.

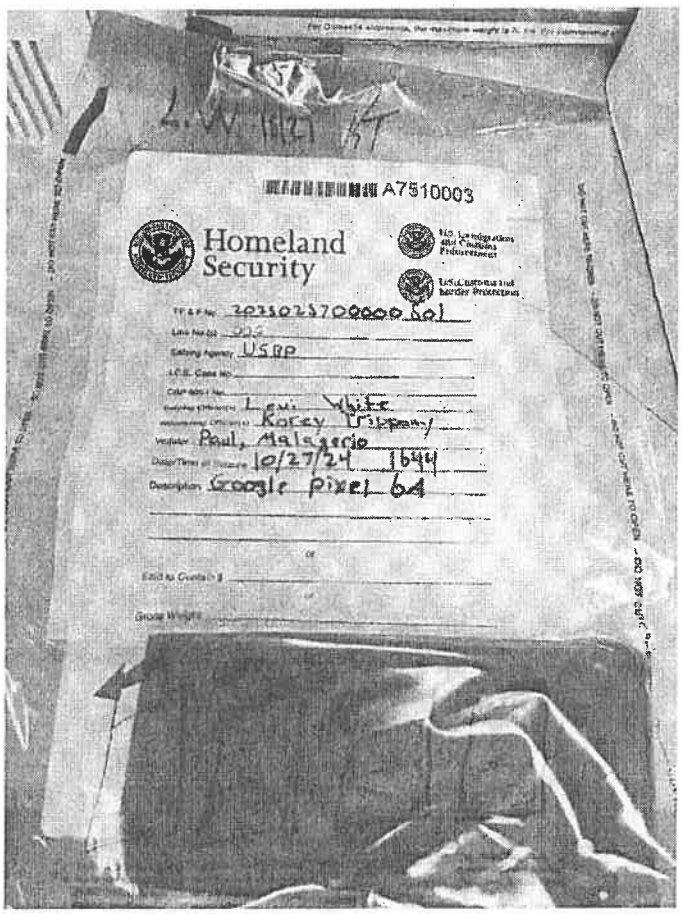
Honorable Gary L. Favro
United States Magistrate Judge

ATTACHMENT A

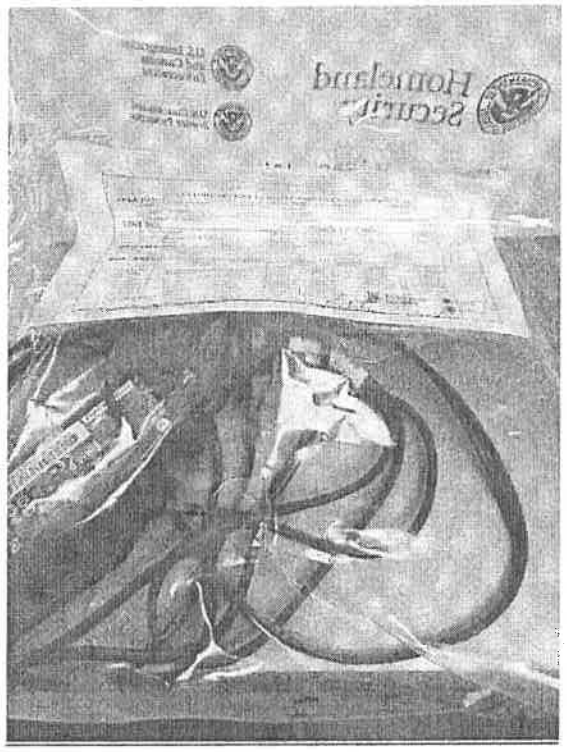
Property to be Searched

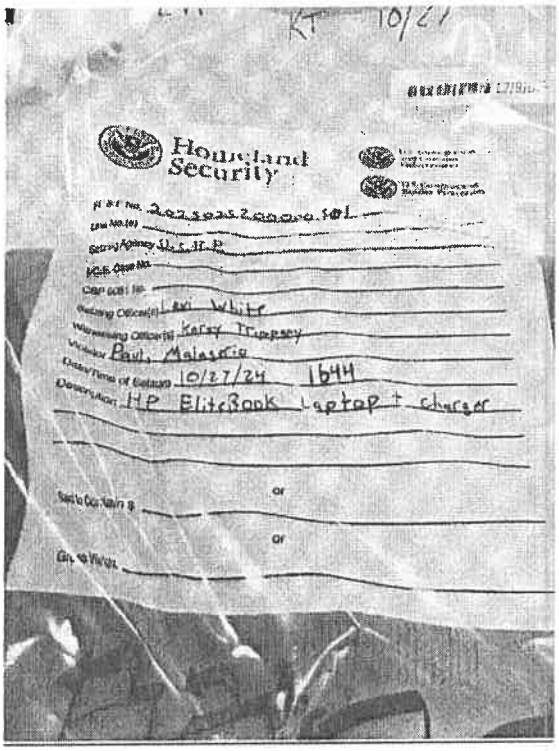
This warrant applies to the following electronic devices (collectively, the "Subject Devices"), to include any attached computer or electronic storage media including SD cards, both of which are currently in the custody of the United States Border Patrol at 135 Trippany Road, Massena, New York 13662. This warrant authorizes the forensic examination of the Subject Devices for the purpose of identifying the electronically stored information described in Attachment B.

a. One (1) Google Pixel 6A cell phone ("Device A"), seized from Paul MALAGERIO;



b. One (1) HP Elitebook Laptop ("Device B"), seized from Paul MALGERIO.





ATTACHMENT B

Items to be Seized and Searched

1. All evidence, fruits, contraband, and/or instrumentalities of violations of Title 8, United States Code, Section 1326(a) and (b)(2) (illegal re-entry of a removed alien with a prior conviction for an aggravated felony), those violations involving Paul MALAGERIO, and specifically the following from the Subject Devices, described with specificity in Attachment A, including deleted data, remnant data, or data contained within slack space:

a. Text messages, instant messages, chat room messages, emails, voice mail messages, and/or other communications relating to illegal international border crossings;

b. Records regarding any calls made or received;

c. Any photographs or audio recordings that relate to illegal international border crossings

d. Geolocation, mapping, and GPS records including information recording schedules or travel;

e. Records of, or information about, any Internet activity including records of Internet Protocol addresses used, firewall logs, caches, browser history, cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

f. Evidence indicating the device user's state of mind as it relates to the crimes under investigation;

g. Evidence of the attachment to the device or of the device to other storage devices or similar containers for electronic evidence;

h. Evidence of counter-forensic programs (and associated data) that are designed to restrict access to, facilitate concealment of, or eliminate data from the device.

2. Evidence of user attribution showing who used or owned the Subject Devices at the time the things described in this warrant were created, edited, or deleted, including:

a. Logs, phonebooks, saved usernames and passwords, documents and browsing history to include Internet Protocol addresses used, internet activity, firewall logs, cashes, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-type web addresses.

b. Evidence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as the evidence of the presence or absence of security software designed to detect malicious software;

c. Evidence of the lack of such malicious software;

d. Evidence indicating how and when the device was accessed or used to determine the chronological context of device access, use, and events relating to the crimes under investigation and to the device user.

3. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

4. During the search of the Subject Devices as described above, photographs may be taken to record the condition thereof.